UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/804,320	03/12/2001	Frank S. Caccavale	10830.0075.NPUS00	1069

27927 7590 11/02/2004

RICHARD AUCHTERLONIE
NOVAK DRUCE LLP
1615 L ST NW
SUITE 850
WASHINGTON, DC 20036

EXAMINER	
TRUONG, THANHNGA B	

ART UNIT	PAPER NUMBER
2135	5

DATE MAILED: 11/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/804,320	CACCAVALE, FRANK S.	
	Examiner	Art Unit	
	Thanhnga Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 March 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 March 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-7, 9, 12-15, 18, 20-26, 28, 31, 38-39 are rejected under 35 U.S.C. 102(b) as being anticipated by Chen et al (US 5,960, 170).

a. *Referring to claim 1:*

i. Chen teaches:

(1) the first file server responding to a request from the client for access to the file in the first file server by determining that an anti-virus scan of the file should be performed, and initiating the anti-virus scan of the file by sending to the second file server a request for the anti-virus scan including a specification of the file **[i.e., viruses are iteratively detected at a client computer. A substantial portion of the tools and information required for the detection and treatment of viruses is provided in a centralized location such as a server, preferably an internet or world wide web server. This virus detection server operates in conjunction with a client to determine whether viruses reside at the client. A virus scan is initiated when a request is received or directed at the virus detection server. The request is direct or can be initiated by various triggering events, such as a programmed request from the client that does not require ongoing user initiation such that the scan is initiated without a request that it apparent to the user (column 2, line 62 through column 3, line 7). In addition, referring to Figure 2, in an initial step 205, a request for a virus scan is received, typically from a source external to the virus detection server 400 such as a client to be scanned. After receipt of the request, in step 210 it is determined by the virus detection server 400 whether a scan is to be**

performed. Preferably, a validation of the virus scan request is performed pursuant to the determination of whether a scan is to be performed (column 6, lines 34-40)], and then

(2) the second file server responding to the request for the anti-virus scan by invoking the virus checker program to perform an anti-virus scan of the specified file by obtaining file data of the file from the first file server and storing the file data of the file into the random access memory of the second file server and performing the anti-virus scan upon the file data of the file in the random access memory **[i.e., referring to Figures 4A, the memory 414 is preferably configured to include routines for the iterative detection of viruses. The configurations are described in further detail with reference to the iterative virus detection module 450a of Figure 4B. Referring now to Figure 4B, an embodiment of an iterative virus detection module ("IVDM") 450b in accordance with Chen's invention is shown to include a scanning module 454, a virus pattern module 456, a virus rules module 458, a cleaning module 460, a cleaning pattern module 462, an access managing module 464, and an access data module 466. The iterative virus detection module 450b, and its referenced modules, includes routines for receiving virus detection requests, validating requests, producing virus detection and treatment objects, receiving the results of the execution of the virus detection and treatment objects, and using the results to produce additional virus detection and treatment objects to ultimately detect viruses and treat them. The iterative virus detection module 450b is typically implemented in software, but can also be implemented in hardware or firmware (column 10, lines 52-67)].**

b. *Referring to claim 2:*

i. Chen further teaches:

(1) wherein the first file server determines that the anti-virus scan of the file should be performed when the client requests the first file server to open the file and the first file server finds that the file has not been checked for viruses **[i.e., referring to Figure 2 again, in an initial step 205, a request for a virus scan is received, typically from a source external to the virus detection server 400 such**

as a client to be scanned. After receipt of the request, in step 210 it is determined by the virus detection server 400 whether a scan is to be performed. Preferably, a validation of the virus scan request is performed pursuant to the determination of whether a scan is to be performed. Continuing with a typical example, the request can be provided by the client 300 in the form a request directed to the virus detection server 400, whereupon the virus detection server 400 can validate the request before proceeding with the determination of whether a virus is associated with the client 300. Preferably, request validation is made by reference to information stored at or accessible to the virus detection server 400 (column 6, lines 34-48; and column 7, lines 4-61 for further details)].

c. *Referring to claims 3-6, 21-25, 39:*

i. These claims have limitations that is similar to those of claim 2, thus they are rejected with the same rationale applied against claim 2 above.

d. *Referring to claim 7:*

i. Chen further teaches:

(1) wherein the first file server maintains in nonvolatile memory an indication of files that have not been checked for viruses, an indication of files that are in the process of being checked, and an indication of files that have been found to contain viruses **[i.e., an exemplary indexing of virus signatures and the preferred signature scanning technique are now described with reference to Figure 4c-4d. Referring to Figure 4c, an exemplary data table 475 is shown to include columns for platform, virus type, and virus identification. In the exemplary table 475, each row includes information about a particular virus. The information can be used to determine whether a scanning routine corresponding to the particular virus will be implemented. Of course, various scanning routines will correspond to groups of viruses with common characteristics. The data table 475 provides an example of how various virus information is indexed. Various additional or alternative criteria for determining which scanning and treatment routines to use can be provided. Preferably, information such as that provided in the exemplary data table 475 is provided in memory 414 for access by the IVDM**

450a in the selection of virus scanning and treatment routines and, more specifically, in the production of virus detection and treatment objects (column 12, line 54 through column 13, line 5)].

e. *Referring to claim 9:*

i. Chen further teaches:

(1) wherein the second file server receives the request for the anti-virus scan and indirectly invokes the virus checker program by reporting a file access event to an operating system of the second file server, and the operating system of the file server responds by invoking the virus checker program to perform the anti-virus scan of the file **[i.e., referring to Figure 5, the request can be initiated directly by a client 300 which accesses the virus detection server 400 using conventional network communication protocols. Although the triggering event 502 that prompts the request 505 is typically initiated directly by the user of the client 300, the request can alternatively be initiated by a triggering event other than user prompting or initiation. This allows for regular virus scanning without requiring user input. Additionally, a group of computers that a user might seek to manage, such as a plurality of computers residing on a LAN, can be subjected to regular virus scanning without requiring user initiation and with minimal use of network resources (column 16, lines 6-17)].**

f. *Referring to claim 12:*

i. Chen further teaches:

(1) wherein the data processing system includes at least a third file server coupled to the first file server for data access of the third file server to the file in the first file server, the third file server also being programmed with a virus checker program that is executable by the third file server to perform an anti-virus scan upon file data in random access memory of the third file server, wherein the first file server performs a load balancing procedure to select one of at least the second file server or the third file server to perform an anti-virus scan of the file when the first file server determines that an anti-virus scan of the file should be performed **[i.e., additionally, a group of computers that a user might seek to manage, such as a**

plurality of computers residing on a LAN, can be subjected to regular virus scanning without requiring user initiation and with minimal use of network resources (column 16, lines 15-17)].

g. *Referring to claim 13:*

i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

h. *Referring to claims 14, 18:*

i. These claims have limitations that is similar to those of claims 2 and 3, thus they are rejected with the same rationale applied against claims 2 and 3 above.

i. *Referring to claims 15, 28:*

i. These claims have limitations that is similar to those of claim 9, thus they are rejected with the same rationale applied against claim 9 above.

j. *Referring to claim 20:*

i. Chen teaches:

(1) at least one client; a first file server coupled to the client for access of the client to at least one file in the first file server **[i.e., referring to Figure 7, an exemplary network communication system 700 includes a local area network (LAN) with clients 300c, a gateway server 710 and an administrative server 750 (column 24, lines 21-24)]**; and

(2) at least a second file server coupled to the first file server for data access of the second file server to the file in the first file server, the second file server being programmed with a virus checker program, the virus checker program being executable by the second file server to perform an anti-virus scan upon file data in random access memory of the second file server; wherein the first file server is programmed to respond to a request from the client for access to the file in the first file server by determining that an anti-virus scan of the file should be performed, and initiating the anti-virus scan of the file by sending to the second file server a request for the anti-virus scan including a specification of the file; and the second file server is programmed to respond to the request for the anti-virus scan by invoking the virus

checker program to perform an anti-virus scan of the specified file by obtaining file data of the file from the first file server and storing the file data of the file in the random access memory of the second file server and performing the anti-virus scan upon the file data in the random access memory **[i.e., these limitations are similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above].**

k. *Referring to claim 26:*

i. This claim has limitations that is similar to those of claim 7, thus it is rejected with the same rationale applied against claim 7 above.

l. *Referring to claim 31:*

i. This claim has limitations that is similar to those of claim 12, thus it is rejected with the same rationale applied against claim 12 above.

m. *Referring to claim 38:*

i. This claim has limitations that is similar to those of claim 20, thus it is rejected with the same rationale applied against claim 20 above.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chen, and further in view of Cassagnol et al (US 6,385,727 B1).

a. *Referring to claim 10:*

i. Chen teaches the claimed subject matter, however Chen does not explicitly mention:

(1) processes executing in a user mode and processes executing in a kernel mode

ii. However, Cassagnol teaches:

(1) In some embodiments, the first processor has a kernel mode of operation and a user mode of operation, and the kernel mode and the user mode define separate security cells. In such embodiments, the first processor preferably executes non-secure software in the user mode of operation and secure software in the kernel mode of operation **(column 3, lines 25-30).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) mention or include the two security cells, user mode and kernel mode (in Chen's CPU 802 of Figure 8A), since the CPU 802 performs functions under the guidance and control provided by instructions received from memory 804, the functions including communications through network media 812 using the network interface 810 **(column 24, lines 46-50 of Chen).**

iv. The ordinary skilled person would have been motivated to:

(1) mention or include the two security cells, user mode and kernel mode (in Chen's CPU 802 of Figure 8A), because Computer viruses continue to be problematic to computers and computer users. Such viruses are typically found within computer programs, files, or code and can produce unintended and sometimes damaging results **(column 1, lines 13-15 of Chen).**

5. Claims 8, 11, 16, 17, 19, 27, 29-30, 32-37, 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chen, and further in view of Cassagnol et al (US 6,385,727 B1), Lam et al (US 6,385,727 B1), and Tzelnic et al (US 5,948,062).

a. *Referring to claim 8:*

i. Chen teaches the claimed subject matter except for:

(1) wherein the request for the anti-virus scan including a specification of the file is an Open Network Computing Remote Procedure Call.

ii. However, Lam teaches:

(1) Communications between a client and a server over heterogeneous network 100 require a method for transporting requests over network 100 from a client running under one operating system to a server that is either running under another operating system, or the same operating system. One widely used

method for communication over heterogeneous network 100 is a remote procedure call (RPC). Techniques for implementing client/server applications, and client/server applications with remote procedure calls are known to those skilled in the art. A remote procedure call (RPC) hides the physical structure of network 100 and makes a server on network 100 appear to be one function call away. Specifically, a remote procedure call hides the details of network 100 by using a procedure call mechanism that is well known **(column 1, lines 44-58).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include the remote procedure call (in Chen's invention) for performing operations over a network, such as network 100, is a client/server architecture **(column 1, lines 28-30 of Lam).**

iv. The ordinary skilled person would have been motivated to:

(1) allow a client to interoperate with one or more servers on other computing platforms, even when the client and server are from different vendors with different operating systems **(column 1, lines 64-66 of Lam).**

b. *Referring to claim 11:*

i. Chen further teaches

(1) wherein an input/output manager in the operating system of the second file server receives a file access call from the virus checker initiator driver, and responds by directing a report of the file access event to the virus checker program **[i.e., referring to Figures 4A, the memory 414, that is considered to include "input/output manager", is preferably configured to include routines for the iterative detection of viruses. The configurations are described in further detail with reference to the iterative virus detection module 450a of Figure 4B (column 10, lines 27-30)].**

ii. However, Chen does not explicitly mention:

(1) the role of input/output manager

iii. Whereas, Lam teaches:

(1) Network stack 425 transmits the packaged function call to server RPC command module 424. Server RPC command module 424 extracts the function call from the packaged request. If the function call is an administration function call, server RPC command module 424 processes the administration function call and replies to RPC command client 414 that in turn communicates with remote client application 411. However, if the function call is an IOMAPI function call, server RPC command module 424 passes the function call to server IPC module 423 Server IPC module 423 transfers the specified function call via a message buffer IPC.sub.--MESSAGE to an I/O manager 430 with an interface to server IPC module 423 **(column 4, lines 1-13).**

iv. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) clearly disclose the role of input/output manager (in Chen's servers) to perform the called management function and returns the result to server IPC module **(column 4, lines 18-19 of Lam).**

v. The ordinary skilled person would have been motivated to:

(1) clearly disclose the role of input/output manager (in Chen's servers) to eliminate problems associated with differing versions of the remote procedure call process on a client and a server **(column 6, lines 47-49 of Lam).**

c. *Referring to claim 16:*

i. Chen teaches:

(1) a server for virus checking executing in the second server in the user mode receives from the network a request for the anti-virus scan upon the file **[i.e., the virus detection server 400 includes a CPU 412, memory 414, a data storage device 416 such as a hard disk, I/O ports 418 and a network interface 420 (column 10, lines 20-23)],** and then

(2) the server for virus checking forwards the request to a virus checker initiator driver executing in the second server in the kernel mode, and the virus checker initiator driver responds to receipt of the request by sending a file access call to the input/output manager **[i.e., the virus detection server 400 includes a CPU**

412, memory 414, a data storage device 416 such as a hard disk, I/O ports 418 and a network interface 420 (column 10, lines 20-23)], and then

(3) the input/output manager responds to the file access call by directing a report of a file access event to a virus checker program executing in the second server in the user mode, and the virus checker program responds by obtaining file data from the file in the first server and storing the file data in random access memory in the second server, and performing an anti-virus scan upon the file data in the random access memory in the second server **[i.e., these limitations are similar to those of claims 1 and 11, thus they are rejected with the same rationale applied against claims 1 and 11 above].**

ii. However, Chen does not explicitly mention:

(1) processes executing in a user mode and processes executing in a kernel mode.

(2) the role of input/output manager

iii. Whereas, Cassagnol teaches:

(1) In some embodiments, the first processor has a kernel mode of operation and a user mode of operation, and the kernel mode and the user mode define separate security cells. In such embodiments, the first processor preferably executes non-secure software in the user mode of operation and secure software in the kernel mode of operation **(column 3, line 25-30).**

iv. and, Lam teaches:

(1) Network stack 425 transmits the packaged function call to server RPC command module 424. Server RPC command module 424 extracts the function call from the packaged request. If the function call is an administration function call, server RPC command module 424 processes the administration function call and replies to RPC command client 414 that in turn communicates with remote client application 411. However, if the function call is an IOMAPI function call, server RPC command module 424 passes the function call to server IPC module 423 Server IPC module 423 transfers the specified function call via a message buffer IPC.sub.--

MESSAGE to an I/O manager 430 with an interface to server IPC module 423 **(column 4, lines 1-13).**

v. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) mention or include the two security cells, user mode and kernel mode (in Chen's CPU 802 of Figure 8A), since the CPU 802 performs functions under the guidance and control provided by instructions received from memory 804, the functions including communications through network media 812 using the network interface 810 **(column 24, lines 46-50 of Chen).**

(2) clearly disclose the role of input/output manager (in Chen's servers) to perform the called management function and returns the result to server IPC module **(column 4, lines 18-19 of Lam).**

vi. The ordinary skilled person would have been motivated to:

(1) mention or include the two security cells, user mode and kernel mode (in Chen's CPU 802 of Figure 8A), because Computer viruses continue to be problematic to computers and computer users. Such viruses are typically found within computer programs, files, or code and can produce unintended and sometimes damaging results **(column 1, lines 13-15 of Chen).**

(2) clearly disclose the role of input/output manager (in Chen's servers) to eliminate problems associated with differing versions of the remote procedure call process on a client and a server **(column 6, lines 47-49 of Lam).**

d. *Referring to claim 19:*

i. This claim has limitations that is similar to those of claim 16, thus it is rejected with the same rationale applied against claim 16 above.

e. *Referring to claim 27:*

i. This claim has limitations that is similar to those of claim 8, thus it is rejected with the same rationale applied against claim 8 above.

f. *Referring to claim 29:*

i. This claim has limitations that is similar to those of claim 10, thus it is rejected with the same rationale applied against claim 10 above.

g. *Referring to claim 30:*

i. This claim has limitations that is similar to those of claim 11, thus it is rejected with the same rationale applied against claim 11 above.

h. *Referring to claims 34, 37:*

i. These claims have limitations that is similar to those of claims 1, 16, and 20, thus they are rejected with the same rationale applied against claims 1, 16, and 20 above.

h. *Referring to claim 40:*

i. This claim has limitations that is similar to those of claim 16, thus it is rejected with the same rationale applied against claim 16 above.

i. *Referring to claim 17:*

i. Chen teaches the claimed subject matter except for:

(1) a data mover in the network file server

ii. However, Tzelnic teaches:

(1) Figure 11 show a block diagram of a preferred implementation of the file manager software 99a for caching of file directory information in each of the data movers, such as the data mover 21a. The file manager 99a includes a network file manager program 141 and a data mover file manager program 142. The network file manager program 141 is a conventional network file manager program that is modified for use with the data mover file manager program 142 **(column 14, lines 15-23).**

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include such data mover for network file access (in Chen's invention) to perform the file system tasks such as managing the file directory for mapping of file names to logical blocks and for locking and unlocking of the files in order to minimize loading on the cached disk array **(column 2, lines 22-26 of Tzelnic).**

iv. The ordinary skilled person would have been motivated to:

(1) include such data mover for network file access (in Chen's invention) since the network attachment, for example, is a computer

programmed to communicate with clients on a network by following a network communication protocol, and to communicate with the integrated cached disk array by issuing channel commands. Although this approach has the advantage of using a conventional integrated cached disk array, the capabilities of the integrated cached disk array are under utilized in this configuration, because the network attachment is a bottleneck to data access **(column 1, line 62 through column 2, line 4 of Tzelnic).**

j. *Referring to claim 32:*

i. This claim has limitations that is similar to those of claims 17 and 20, thus it is rejected with the same rationale applied against claims 17 and 20 above.

k. *Referring to claims 33, 36:*

i. These claims have limitations that is similar to those of claim 14, thus they are rejected with the same rationale applied against claim 14 above.

l. *Referring to claim 35:*

i. This claim has limitations that is similar to those of claims 17, 20, 32, thus it is rejected with the same rationale applied against claim 16 above.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Ji et al (US 5, 623, 600) discloses A system for detecting and eliminating viruses on a computer network includes a File Transfer Protocol (FTP) proxy server, for controlling the transfer of files and a Simple Mail Transfer Protocol (SMTP) proxy server for controlling the transfer of mail messages through the system (see abstract).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and

phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

TBT
October 30, 2004

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100